AMENDMENTS TO THE CLAIMS

This listing of claims replaces all prior versions and listing of claims in this application.

Claim 1. (*Currently Amended*) A method for transferring a first~~electronic~~ root key between a key provider system and a second other system via an information network comprising the steps of:

a) encrypting the first~~electronic~~ root key using a first~~encryption~~ super-root key of the key provider system;

b) providing within the second other system a first secure module having a second ~~encryption~~ super-root key within a read-only memory circuit thereof and provided with the first secure module, the second~~encryption~~ super-root key accessible only by program code being executed on a processor internal to the first secure module, and wherein the second~~encryption~~ super-root key is other than modifiable and other than accessible outside of the module;

c) transferring the encrypted first~~electronic~~ root key from the key provider system to the second other system via the information network;

d) providing the encrypted first~~electronic~~ root key to the processor internal to the first secure module of the second other system; and,

e) executing program code on the processor internal to the first secure module to decrypt the encrypted first~~electronic~~ root key using the second~~encryption~~ super-root key stored within the read-only memory circuit of the first secure module and to store the decrypted first~~electronic~~ root key internally within a secure key memory location of the first secure module, wherein the first root key is useable for at least one of encrypting and decrypting private keys, and wherein a bit length of

the first super-root key is greater than a bit length of the first root key, and said bit length of the first root key is greater than a bit length of any of said private keys.

Claim 2. (*Previously Presented*) The method according to claim 1 wherein the processor internal to the module accesses the second~~encryption~~ super-root key only for decrypting encrypted~~electronic~~ root keys, wherein the decrypted ~~electronic~~ root keys are then stored within the module inaccessible outside the secure module.

Claim 3. (*Original*) The method according to claim 2 wherein the step (a) is performed in a corresponding secure module.

Claim 4. (*Previously Presented*) The method according to claim 3 wherein the processor internal to the module accesses the second~~encryption~~ super-root key only in response to a request from a corresponding secure module.

Claim 5. (*Previously Presented*) The method according to claim 4 wherein the second ~~encryption~~ super-root key and the first~~encryption~~ super-root key are the private and public portions of an asymmetric private/public-key pair, respectively.

Claim 6. (*Previously Presented*) The method according to claim 4 wherein the second ~~encryption~~super-root key and the first ~~encryption~~super-root key are a same private key for use with a symmetric key-based encryption algorithm.

Claim 7. (*Previously Presented*) The method according to claim 6 comprising the additional step prior to step a) of:

a1) generating a first ~~electronic~~root key within a key-generating processor internal to the key provider system.

Claim 8. (*Original*) The method according to claim 7 wherein the key-generating processor is embodied on the corresponding secure module.

Claim 9. (*Currently Amended*) The method according to claim 6 wherein the first~~electronic~~ root key is~~is a root key for use~~ useable for ~~in~~ at least one of encrypting and decrypting private encryption keys.

Claim 10. (*Currently Amended*) A method for transferring a first ~~electronic~~root key between a key provider system and a second other system via an information network comprising the steps of:

a) encrypting the first ~~electronic~~root key using a first ~~encryption~~super-root key of the key provider system;

b) providing within the second other system a first secure module having second and third ~~encryption~~super-root keys within a memory circuit thereof, the second and third ~~encryption~~super-root keys accessible only by program code being executed on a processor internal to the first secure module for decrypting encrypted ~~electronic~~root keys and for storing the decrypted ~~electronic~~root keys within a memory circuit of the first secure module, and wherein the second and third ~~encryption~~super-root keys are other than accessible outside of the module;

c) transferring the encrypted first ~~electronic~~root key from the key provider system to the second other system via the information network;

d) providing the encrypted first ~~electronic~~root key to the processor internal to the first secure module of the second other system; and,

e) executing program code on the processor internal to the first secure module to decrypt the encrypted first ~~electronic~~root key using the second ~~encryption~~super-root key stored within the memory circuit of the first secure module and to store the decrypted first ~~electronic~~root key internally within a secure key memory location of the first secure module, wherein the first root key is useable for at least one of encrypting and decrypting private keys, and wherein a bit length of the first super-root key is greater than a bit length of the first root key, and said bit length of the first root key is greater than a bit length of any of said private keys.

Claim 11. (*Previously Presented*) A method for transferring a first ~~electronic~~root key between a key provider system and a second other system via an information network according to claim 10 comprising the steps of:

f) encrypting a fourth ~~encryption~~super-root key using one of the third ~~encryption~~super-root key and a key corresponding to the third ~~encryption~~super-root key;

g) transferring the encrypted fourth ~~encryption~~super-root key from the key provider system to the second other system via the information network;

h) providing the encrypted fourth ~~encryption~~super-root key to the processor internal to the first secure module of the second other system; and,

i) executing program code on the processor internal to the first secure module to decrypt the encrypted fourth ~~encryption~~super-root key using the third ~~encryption~~super-root key stored within the memory circuit of the first secure module and to store the decrypted fourth ~~encryption~~super-root key within the memory circuit of the first secure module at a location corresponding approximately to the location where the second ~~encryption~~super-root key was stored.

Claim 12. (*Previously Presented*) The method according to claim 11 wherein the second and third ~~encryption~~super-root keys are only replaceable through use of another of the second and third ~~encryption~~super-root keys.

Claim 13. (*Previously Presented*) The method according to claim 12 wherein the second, third and fourth ~~encryption~~super-root keys are~~super-root keys~~ useable for at least one of encrypting and decrypting root keys.

Claim 14. (*Previously Presented*) The method according to claim 11 wherein the step of storing the decrypted fourth ~~encryption~~super-root key comprises the steps of:

i1) erasing the second ~~encryption~~super-root key from a first storage area of the memory circuit; and,

i2) storing the decrypted fourth ~~encryption~~super-root key within approximately the same first storage area of the same memory circuit.

Claim 15. (*Previously Presented*) A system for transferring a secure ~~electronic~~root key between a key provider system and a second other system via an information network that is other than secure comprising a secure module in operative communication with the second other system, the secure module including:

an encryption processor;

an input port for receiving encrypted electronic data from outside the module and for providing the encrypted electronic data to the encryption processor;

a memory circuit in operative communication with the encryption processor for storing at least a first ~~encryption~~super-root key;

memory storage having program code stored therein and executable on the encryption processor for, upon receipt of an encrypted secure ~~electronic~~root key, decrypting the encrypted

secure ~~electronic~~root key using the at least a first ~~encryption~~super-root key and for storing the decrypted secure ~~electronic~~root key within the memory circuit, the at least a first ~~encryption~~super-root key being other than accessible by any code other than the program code and being other than modifiable thereby, wherein the secure root key is useable for at least one of encrypting and decrypting private keys, and wherein a bit length of the first super-root key is greater than a bit length of the secure root key, and said bit length of the secure root key is greater than a bit length of any of said private keys.

Claim 16. (*Previously Presented*) The system according to claim 15 wherein the code executable on the encryption processor accesses the at least a first ~~encryption~~super-root key only in response to a request from a corresponding secure module.

Claim 17. (*Original*) The system according to claim 16 wherein the code executable on the encryption processor is only for performing encryption functions the results of which are inaccessible outside of the module.

Claim 18. (*Previously Presented*) The system according to claim 17 wherein the memory circuit for storing the at least a first ~~encryption~~super-root key is a read-only memory circuit.

Claim 19. (*Original*) The system according to claim 18 wherein the module is FIPS 140 compliant.

Claim 20. (*Previously Presented*) The system according to claim 19 wherein the module includes a tamper detection circuit for erasing the first~~cryptographic~~ super-root key in dependence upon a detected attempt to access the electronic contents of the module in an unauthorized fashion.

Claim 21. (*Previously Presented*) A system for transferring a secure ~~electronic~~root key between a key provider system and a second other system via an information network that is other than secure comprising a secure module in operative communication with the second other system, the secure module including:

an encryption processor;

an input port for receiving encrypted electronic data from outside the module and for providing the encrypted electronic data to the encryption processor;

a memory circuit in operative communication with the encryption processor for storing a first ~~encryption~~super-root key within a first memory location thereof and for storing a second ~~encryption~~super-root key within a second other memory location thereof;

memory storage having program code stored therein and executable on the encryption processor for, upon receipt of an encrypted third ~~encryption~~super-root key from the second other system, decrypting the encrypted third ~~encryption~~super-root key using one of the first and second ~~encryption~~super-root keys and for storing the decrypted third ~~encryption~~super-root key at a memory location corresponding to the other one of the first and second ~~encryption~~super-root keys, the first

and second ~~encryption~~super-root keys being ~~other than~~ accessible only by ~~any code other than~~ the program code and being ~~other than~~ modifiable ~~absent erasing thereof~~ only by ~~any code other than~~ the program code for all modifications excluding erasure, wherein the secure root key is useable for at least one of encrypting and decrypting private keys, and wherein a bit length of the first super-root key is greater than a bit length of the secure root key, and said bit length of the secure root key is greater than a bit length of any of said private keys.

Claim 22. (*Original*) The system according to claim 21 wherein the code executable on the encryption processor accesses the first and second ~~encryption~~super-root keys only in response to a request from a corresponding secure module.

Claim 23. (*Original*) The system according to claim 22 wherein the code executable on the encryption processor is only for performing encryption functions the results of which are inaccessible outside of the module.

Claim 24. (*Previously Presented*) The system according to claim 23 wherein the memory circuit for storing the first and second ~~encryption~~super-root keys is a substantially non-volatile reprogrammable memory circuit.

Claim 25. (*Previously Presented*) The system according to claim 24 wherein the substantially non-volatile reprogrammable memory circuit is one of an electrically erasable programmable read-only memory (EEPROM) circuit and a random access memory (RAM) circuit having an on-board power supply in the form of a battery.

Claim 26. (*Original*) The system according to claim 25 wherein the module is FIPS 140 compliant.

Claim 27. (*Original*) The system according to claim 26 wherein the module includes a tamper detection circuit for erasing every cryptographic key stored within the memory circuit in dependence upon a detected attempt to access the electronic contents of the module in an unauthorized fashion.

Claim 28. (*New*) The method according to claim 1 wherein the bit length of the first super-root key is between about 2048 bits and about 4096 bits, the bit length of the first root key is between about 512 bits and about 2048 bits, and the bit length of any of said private keys is between about 128 bits and about 1024 bits.

Claim 29. (*New*) The method according to claim 10 wherein the bit length of the first super-root key is between about 2048 bits and about 4096 bits, the bit length of the first root key is between about 512 bits and about 2048 bits, and the bit length of any of said private keys is between about 128 bits and about 1024 bits.

Claim 30. (*New*) The system according to claim 15 wherein the bit length of the first super-root key is between about 2048 bits and about 4096 bits, the bit length of the first root key is between about 512 bits and about 2048 bits, and the bit length of any of said private keys is between about 128 bits and about 1024 bits.

Claim 31. (*New*) The system according to claim 21 wherein the bit length of the first super-root key is between about 2048 bits and about 4096 bits, the bit length of the first root key is between about 512 bits and about 2048 bits, and the bit length of any of said private keys is between about 128 bits and about 1024 bits.